p.14683-A

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　４月　２日

出願番号
Application Number: 特願２００１－１０３０６６

出願人
Applicant(s): 日本電信電話株式会社

２００１年　６月１３日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０５５４３７

【書類名】　特許願

【整理番号】　NTTH127204

【提出日】　平成13年 4月 2日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/62

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　斎藤　賢一

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　重松　智志

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　羽田野　孝裕

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　藤井　孝治

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　中西　衛

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　池田　奈美子

出証特２００１－３０５５４３７

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100064621

【弁理士】

【氏名又は名称】　山川　政樹

【電話番号】　03-3580-0961

【手数料の表示】

【予納台帳番号】　006194

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9701512

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　生体情報認証自動現金受け払い機

【特許請求の範囲】

【請求項１】　利用者の生体情報の認証に基づき前記利用者に対し現金の受け払いを含むサービスを提供する生体情報認証自動現金受け払い機であって、

利用者の生体情報に基づき利用者本人の認証を行う生体情報認証トークンを備え、

前記生体情報認証トークンは、

利用者の生体情報を記憶する記憶手段と、

利用者の生体情報を検出するセンサと、

前記センサの検出情報と前記記憶手段の記憶情報との一致に基づき制御情報を出力する処理手段とを有し、

前記生体情報認証自動現金受け払い機は、

前記処理手段の制御情報に基づいて前記利用者に前記サービスを提供するサービス提供手段を有することを特徴とする生体情報認証自動現金受け払い機。

【請求項２】　請求項１において、

予め利用者の口座番号に対応して残高が記憶されたデータベースを備え、

前記生体情報認証トークンの記憶手段には前記利用者の口座番号が記憶され、

前記処理手段は、前記センサの検出情報と記憶手段の記憶情報との一致に基づき前記記憶手段の口座番号を前記制御情報として出力し、

前記サービス提供手段は、

前記処理手段からの口座番号を受信すると前記データベース内の受信口座番号に対応する残高を取得する取得手段と、

前記取得手段により取得された残高から利用者の所定操作に応じた現金を引き出す引き出し手段と、

前記取得手段により取得された残高から前記引き出し手段により引き出された金額を減じて新たな残高として前記データベースに記憶する残高記録手段と

を有することを特徴とする生体情報認証自動現金受け払い機。

【請求項３】　請求項１において、

予め利用者の口座番号に対応して残高が記憶されたデータベースを備え、

前記生体情報認証トークンの記憶手段には前記利用者の口座番号が記憶され、

前記処理手段は、前記センサの検出情報と記憶手段の記憶情報との一致に基づき前記記憶手段の口座番号を前記制御情報として出力し、

前記サービス提供手段は、

前記処理手段からの口座番号を受信すると前記データベース内の受信口座番号に対応する残高を取得する取得手段と、

前記取得手段により取得された残高に対し利用者により入金された金額を加算し新たな残高として前記データベースに記憶する残高記録手段と

を有することを特徴とする生体情報認証自動現金受け払い機。

【請求項４】　利用者の生体情報の認証に基づき前記利用者に対し現金の受け払いを含むサービスを提供する生体情報認証自動現金受け払い機であって、

センサにより検出された利用者の生体情報と記憶手段に記憶された生体情報との比較照合に基づき利用者本人を認証する生体情報認証トークンと情報の授受を行う情報授受手段と、

センサの検出情報と記憶手段の生体情報との一致に基づき前記生体情報認証トークンから出力される制御情報が前記情報授受手段により受信されると、この受信制御情報に基づいて前記利用者に前記サービスを提供するサービス提供手段と

を有することを特徴とする生体情報認証自動現金受け払い機。

【請求項５】　請求項４において、

予め利用者の口座番号に対応して残高が記憶されたデータベースを備え、

前記生体情報認証トークンの記憶手段には前記利用者の口座番号が記憶され、

前記サービス提供手段は、

前記センサの検出情報と記憶手段の生体情報との一致に基づき前記生体情報認証手段から前記制御情報として出力される口座番号が前記情報授受手段により受信されると、前記データベース内のこの受信口座番号に対応する残高を取得する取得手段と、

前記取得手段により取得された残高から利用者の所定操作に応じた現金を引き出す引き出し手段と、

前記取得手段により取得された残高から前記引き出し手段により引き出された金額を減じて新たな残高として前記データベースに記憶する残高記録手段と

を有することを特徴とする生体情報認証自動現金受け払い機。

【請求項６】　請求項４において、

予め利用者の口座番号に対応して残高が記憶されたデータベースを備え、

前記生体情報認証トークンの記憶手段には前記利用者の口座番号が記憶され、

前記サービス提供手段は、

前記センサの検出情報と記憶手段の生体情報との一致に基づき前記生体情報認証手段から前記制御情報として出力される口座番号が前記情報授受手段により受信されると、前記データベース内のこの受信口座番号に対応する残高を取得する取得手段と、

前記取得手段により取得された残高に対し利用者により入金された金額を加算し新たな残高として前記データベースに記憶する残高記録手段と

を有することを特徴とする生体情報認証自動現金受け払い機。

【請求項７】　請求項２または３または５または６において、

前記残高記録手段は、利用者の預金通帳が挿入されている場合に前記残高を含む情報を前記預金通帳に記録することを特徴とする生体情報認証自動現金受け払い機。

【請求項８】　請求項１ないし７の何れかにおいて、

前記記憶手段は利用者の指紋画像を前記生体情報として記憶し、

前記センサは利用者の指紋画像を前記生体情報として検出し、

前記処理手段または生体情報認証トークンは、前記センサにより検出された指紋画像と前記記憶手段の指紋画像との一致に基づき前記制御情報を出力することを特徴とする生体情報認証自動現金受け払い機。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、生体情報認証自動現金受け払い機に関する。

【０００２】

【従来の技術】

この種の自動現金受け払い機（以下、ＡＴＭ）は銀行等に設置され、利用者が自身の銀行カードをＡＴＭに挿入し、かつ自身のパスワード（暗証番号）を入力すると、ＡＴＭではその利用者が銀行口座の所有者か否かを判断し、所有者と判断した場合は、利用者のお金の引き出しなど、各種サービスを提供している。

【０００３】

しかし、このようなＡＴＭでは、利用者の銀行カード及びパスワードが盗まれると、第三者により不正に利用され、セキュリティ上の問題があるため、特開昭６３－１２４１７５号公報に開示されているような、利用者の指紋を読み取って利用者本人か否かを認証するようにしたものがある。

【０００４】

このような指紋照合装置付ＡＴＭでは、カードに記憶された登録指紋データをＡＴＭの指紋照合装置で読み込み、この読み込んだ指紋データと、指紋センサにより測定された指紋データとを照合することにより、その利用者が銀行口座の所有者か否かを認証し、所有者と認証した場合は、利用者のお金の引き出しなど、各種サービスを提供している。

【０００５】

【発明が解決しようとする課題】

しかしながら、前記指紋照合装置付ＡＴＭでは、ＡＴＭ内に利用者の登録指紋データが読み込まれるため、指紋データが銀行側に悪用されるのではないかという心配が利用者側に発生するという問題があった。また、指紋センサを複数の利用者が共用で用いるため、直前に利用した利用者の指紋の跡（汗などによって生じる）が指紋センサ上に残っている場合があり、このような指紋センサ上の残存指紋が利用されて容易に偽造指紋が作成されてしまうという問題もあった。

【０００６】

したがって、本発明は、利用者の指紋を読み取って利用者本人か否かを認証し利用者のお金の引き出しなど各種サービスを提供するＡＴＭにおいて、利用者の指紋データのセキュリティを向上させることを目的とする。

【０００７】

【課題を解決するための手段】

このような課題を解決するために本発明は、利用者の生体情報の認証に基づき利用者に対し現金の受け払いを含むサービスを提供する生体情報認証自動現金受け払い機であって、利用者の生体情報に基づき利用者本人を認証する生体情報認証トークンは、利用者の生体情報を記憶する記憶手段と、利用者の生体情報を検出するセンサと、センサの検出情報と記憶手段の記憶情報との一致に基づき制御情報を出力する処理手段とを有し、生体情報認証自動現金受け払い機は、処理手段の制御情報に基づき前記サービスの提供を行うサービス提供手段を有するように構成したものである。

【０００８】

この場合、予め利用者の口座番号に対応して残高が記憶されたデータベースを備え、かつ記憶手段に利用者の口座番号を記憶するとともに、処理手段は、センサの検出情報と記憶手段の記憶情報との一致に基づき記憶手段の口座番号を制御情報として出力し、サービス提供手段は、処理手段からの口座番号を受信するとデータベース内の受信口座番号に対応する残高を取得する取得手段と、取得手段により取得された残高から利用者の所定操作に応じた現金を引き出す引き出し手段と、取得手段により取得された残高から引き出し手段により引き出された金額を減じて新たな残高としてデータベースに記憶する残高記録手段とを有するものである。

【０００９】

また、サービス提供手段は、処理手段からの口座番号を受信するとデータベース内の受信口座番号に対応する残高を取得する取得手段と、取得手段により取得された残高に対し利用者により入金された金額を加算し新たな残高としてデータベースに記憶する残高記録手段とを有するものである。

また、残高記録手段は、利用者の預金通帳が挿入されている場合に前記残高を含む情報を預金通帳に記録するものである。

また、記憶手段に利用者の指紋画像を前記生体情報として記憶し、センサは利用者の指紋画像を前記生体情報として検出するとともに、処理手段は、センサにより検出された指紋画像と記憶手段の指紋画像との一致に基づき制御情報を出力

するように構成したものである。

【００１０】

【発明の実施の形態】

以下、本発明について図面を参照して説明する。

図１は、本発明に係る生体情報認証自動現金受け払い機を適用したシステムの構成を示すブロック図である。図１に示す自動現金受け払い機１０１は、銀行などに設置され、利用者の生体情報として利用者の指紋を照合することにより、利用者本人であるか否かを認証し、利用者本人であると認証すると利用者のお金の引き出しなど、各種サービスを提供するものである。ここで、自動現金受け払い機１０１はネットワーク１１１を介してデータベース１１０に接続される。なお、図１には示されていないが、データベース１１０は、サーバを介してネットワーク１１１に接続されていても良い。

【００１１】

前記自動現金受け払い機１０１は、図１に示すように、後述の指紋認証トークンが差し込まれる差込口１０２が設けられ、かつ前記指紋認証トークンからの指紋情報の認証処理等を行う処理装置１０３が設けられているとともに、処理装置１０３には、記憶装置１０４と、利用者への現金の受け払いを行う現金受け払い制御装置１０５と、差込口１０９に差し込まれた通帳に残高などの記入を行う通帳記入装置１０８とが接続される構成となっている。

【００１２】

この自動現金受け払い機１０１の前記差込口１０２に差し込まれる指紋認証トークンは、利用者が所持し、持ち運びのできる小型、軽量の装置であって、図２に示すように、本体部２０１が設けられているとともに、本体部２０１に、指紋センサ２０２と、処理装置２０３と、記憶装置２０４と、自動現金受け払い機１０１との接続端子である端子２０５とが設けられている。そして、処理装置２０３は、指紋センサ２０２，記憶装置２０４及び端子２０５に接続されている。

【００１３】

図５は前記指紋認証トークン２００を構成する指紋センサ２０２の概略的な断面を示す図である。本指紋センサ２０２は、例えばシリコンからなる半導体基板

２１１上の下層絶縁膜２１２上に形成された層間絶縁膜２１４上に、たとえば８０μｍ角の複数のセンサ電極２１５と、格子状のアース電極２１６とを備え、複数のセンサ電極２１５とアース電極２１６とを、層間絶縁膜２１４表面で規定される同一平面上に配置している。

【００１４】

センサ電極２１５は、層間絶縁膜２１４上に形成されたパシベーション膜２１７で覆い、１５０μｍ間隔に複数個を備えるようにするとともに、Ａｕから構成し、膜厚１μｍ程度に形成している。パシベーション膜２１７の膜厚は３μｍ程度としたので、センサ電極２１５上には、パシベーション膜２１７が約２（＝３－１）μｍ存在している。このパシベーション膜２１７は、例えばポリイミドなどの比誘電率が４．０程度の絶縁物から構成される。

【００１５】

上記下層絶縁膜２１２上には、センサ電極２１５にスルーホールを介して接続する配線２１３を形成する一方、半導体基板２１１上には、センサ電極２１５に形成される容量を検出する容量検出回路２１８を形成している。この容量検出回路２１８は、前述した配線２１３によってセンサ電極２１５に接続される。容量検出回路２１８は、センサ電極２１５毎に用意され、センサ電極２１５と認識対象（指）の一部との間に形成される容量を検出する。

【００１６】

各容量検出回路２１８の出力は、処理装置２０３に接続され、この処理装置２０３により、各センサ電極２１５に形成された容量を濃淡に変換した指紋画像データが生成される。

各容量検出回路２１８、処理装置２０３及び記憶装置２０４は、たとえばセンサ電極２１５下の半導体基板２１１上に形成する。これにより指紋センサ２０２，処理装置２０３及び記憶装置２０４をワンチップ化でき、したがって指紋認証トークン２００のワンチップ化が可能になる。なお、こうしたワンチップ化の他の例として、例えば特開２０００－２４２７７１に開示されたものがある。

【００１７】

図６（ａ）は、容量検出回路２１８の回路図である。図６（ａ）において、Ｃ

ｆは図５におけるセンサ電極２１５と指３の皮膚との間に形成される静電容量である。容量Ｃｆを形成するセンサ電極２１５はＮchＭＯＳトランジスタＱ３ａのドレイン端子に接続されており、このトランジスタＱ３ａのソース端子は電流Ｉの電流源２１ａの入力側に接続されている。また、センサ電極２１５とトランジスタＱ３ａとの節点Ｎ１ａには、ＮchＭＯＳトランジスタ（第１の素子）Ｑ２ａのソース端子が接続されている。このトランジスタＱ２ａのドレイン端子には、ソース端子に電源電圧ＶDDが印加されたＰchＭＯＳトランジスタ（第１のスイッチ手段）Ｑ１ａのドレイン端子と、ドレイン端子に電源電圧ＶDDが印加されソース端子が抵抗Ｒａを介して接地に接続されたＮchＭＯＳトランジスタＱ４ａのゲート端子とが接続されている。このトランジスタＱ４ａのソース端子にインバータゲート４１が接続されている。

【００１８】

各トランジスタＱ１ａ，Ｑ３ａのゲート端子にはそれぞれ信号ＰＲＥ（バー），ＲＥが印加される。また、トランジスタＱ２ａのゲート端子には定電圧源からバイアス電圧ＶＧが印加される。ここで、トランジスタＱ２ａが非導通状態になるゲートーソース間のしきい値電圧をＶthとすると、ＶDD＞ＶＧ－Ｖthとなるように電圧ＶDD，ＶＧが設定される。

また、節点Ｎ１ａ，Ｎ２ａはそれぞれ寄生容量Ｃｐ１ａ，Ｃｐ２ａを有している。

【００１９】

図６（ｂ）～図６（ｄ）は、図６（ａ）に示した容量検出回路２１８の動作を説明するためのタイミングチャートであり、図６（ｂ）はトランジスタＱ１ａを制御する信号ＰＲＥ（バー）の電位変化を示し、図６（ｃ）はトランジスタＱ３ａを制御する信号ＲＥの電位変化を示し、図６（ｄ）は節点Ｎ１ａ，Ｎ２ａそれぞれの電位変化を示している。

最初、トランジスタＱ１ａのゲート端子にはＨｉｇｈレベル（ＶDD）の信号ＰＲＥ（バー）が与えられ、トランジスタＱ３ａのゲート端子にはＬｏｗレベル（ＧＮＤ）の信号ＲＥが与えられている。したがって、このときトランジスタＱ１ａ，Ｑ３ａはともに導通していない。

【００２０】

この状態で信号ＰＲＥ（バー）がＨｉｇｈレベルからＬｏｗレベルに変化すると、トランジスタＱ１ａが導通状態になる。このときトランジスタＱ３ａは非導通状態のままであり、信号発生回路２０は停止状態にあるから、節点Ｎ２ａの電位がＶDDにプリチャージされる。

また、トランジスタＱ２ａのゲートーソース間電圧がしきい値電圧Ｖthに達してトランジスタＱ２ａが非導通状態になるまで、節点Ｎ１ａが充電される。これにより、節点Ｎ１ａの電位がＶＧ－Ｖthにプリチャージされる。

【００２１】

プリチャージが終了した後、信号ＰＲＥ（バー）がＨｉｇｈレベルに変化すると、トランジスタＱ１ａが非導通状態になる。これと同時に信号ＲＥがＨｉｇｈレベルに変化すると、トランジスタＱ３ａが導通状態になり、信号発生回路２０が動作状態に変化する。そして、電流源２１ａにより節点Ｎ１ａに充電された電荷が引き抜かれ、節点Ｎ１ａの電位がわずかに低下すると、トランジスタＱ２ａのゲートーソース間電圧がしきい値電圧Ｖthより大きくなり、トランジスタＱ２ａが導通状態に変化する。これにより節点Ｎ２ａの電荷も引き抜かれ、節点Ｎ２ａの電位低下が開始する。

信号ＲＥをＨｉｇｈレベルにする期間をΔｔとするとΔｔ経過後の節点Ｎ１ａの電位低下ΔＶはＶDD－（ＶＧ－Ｖth）＋ＩΔｔ／（Ｃｆ＋Ｃｐ１ａ）になる。ここで、寄生容量Ｃｐ２ａは寄生容量Ｃｐ１ａに対して十分小さいとしている。

【００２２】

電流源２１ａの電流Ｉと期間Δｔと寄生容量Ｃｐ１ａ，Ｃｐ２ａは、各々一定であるから、電位低下ΔＶは、センサ電極２１５と検出対象である指の表面３との間に発生する容量の値Ｃｆによって決定される。この容量値Ｃｆはセンサ電極２１５と指の表面３との距離によって決まるので、指紋の凹凸によって異なる。このことから、低下電位ΔＶの大きさが、指紋の凹凸を反映して変化する。この電位低下ΔＶが、入力信号として出力回路４０に供給されるので、出力回路４０でΔＶが入力され、指紋の凹凸を反映した信号が出力回路４０から出力される。

こうした各容量検出回路２１８の出力信号が処理装置２０３により処理され、

前述の指紋画像データとして生成される。

【００２３】

次に、以上のように構成された指紋センサ２０２を有する指紋認証トークン２００、及び指紋認証トークン２００の指紋情報の認証に基づき現金の受け払いを行う自動現金受け払い機１０１の動作を図３，図４のフローチャートに基づいて説明する。

（第１の実施の形態）

まず、図３のフローチャートに示す第１の実施の形態の動作から説明する。第１の実施の形態は、利用者の現金引き出しに対応する動作を示すものである。

利用者が自動現金受け払い機１０１から現金の引き出しを行う場合は、ステップＳ１で自身の預金通帳を差込口１０９に差し込む。ここで、利用者が自身の通帳に残高などの記帳が不要な場合はステップＳ１の動作は省略される。続いて利用者は自身の所持する指紋認証トークン２００を差込口１０２に差込み（ステップＳ２）、さらにその指紋認証トークン２００の指紋センサ２０２上に自身の指をのせる（ステップＳ３）。

【００２４】

すると、指紋認証トークン２００の処理装置２０３は、指紋センサ２０２により検出された指紋画像を読み取って画像データとして処理し、その指紋画像データの中から特徴となるデータを照合情報として抽出する（ステップＳ４）。ここで、指紋認証トークン２００の記憶装置２０４には、予め指紋センサ２０２により検出され処理装置２０３により処理された利用者自身の指紋画像データ中の特徴部分を示す照合情報が登録されており、処理装置２０３は、記憶装置２０４に保存されているこの登録情報とステップＳ４で抽出した照合情報とを比較する（ステップＳ５）。

【００２５】

そして、双方の照合情報が不一致の場合はそのまま処理を終了するが、双方の照合情報が一致してステップＳ６の「照合情報が一致？」の判定がＹＥＳとなると、処理装置２０３は、予め記憶装置２０４内に保存されているその利用者の銀行口座番号を自動現金受け払い機１０１の処理装置１０３に送信する（ステップ

Ｓ７）。ここで、データベース１１０内には各利用者の口座番号に対応して残高が記憶されており、自動現金受け払い機１０１の処理装置１０３は指紋認証トークン２００から口座番号が送信されてくると、この口座番号を受信し受信した口座番号に対応する残高をネットワーク１１１を介してデータベース１１０から取得し、記憶装置１０４に記憶する（ステップＳ８）。

【００２６】

そして、利用者がキーボード１０７を操作して自身の引き出し金額を入力すると（ステップＳ９）、自動現金受け払い機１０１の処理装置１０３は、記憶装置１０４に記憶された残高と、利用者の入力操作に基づく引き出し金額との大小を比較する（ステップＳ１０）。ここで、残高が引き出し金額未満でステップＳ１１の「残高が引き出し金額以上か？」の判定がＮＯとなる場合は、そのまま処理を終了するが、残高が引き出し金額以上でありステップＳ１１の判定がＹＥＳとなると、現金受け払い制御装置１０５を制御することにより、引き出し金額に相当する現金を現金受け払い口１０６へ排出させる（ステップＳ１２）。

【００２７】

この場合、自動現金受け払い機１０１の処理装置１０３は、記憶装置１０４に記憶された残高から引き出し金額を差し引いた残高をネットワーク１１１を介してデータベース１１０に書き込む（ステップＳ１３）。その後、利用者による指紋認証トークン２００の差込口１０２からの引き抜きが行われ（ステップＳ１４）、利用者の預金通帳が差し込まれている場合は、処理装置１０３は通帳記入装置１０８を制御して利用者の現金引き出し額などを預金通帳に記録させる（ステップＳ１５）。

【００２８】

このように、第１の実施の形態では、利用者がそれぞれ所有する指紋トークン２００に利用者自身の指紋データを登録するとともに、利用者の口座番号を記憶し、指紋トークン２００の指紋センサ２０２が読み取った指紋データと、登録データとが一致すると、記憶している口座番号を自動現金受け払い機１０１へ送信し、自動現金受け払い機１０１では、この口座番号を受信するとデータベース１１０からこの口座番号に対応する残高を取得し、この残高に応じた現金の払い出

しを行うようにしたものである。この結果、従来の自動現金受け払い機のように、利用者の登録指紋データが内部に読み込まれないため、指紋データが銀行側に悪用されるといった心配を利用者に抱かせるという問題を回避できる。また、従来の自動現金受け払い機のように、指紋センサを複数の利用者が共用で使用されることがないことから、指紋センサ上の残存指紋が第三者により不正に利用されて容易に偽造指紋が作成されてしまうという問題も回避できる。

【００２９】

なお、本実施の形態では、指紋認証トークン２００の記憶装置２０４に、利用者の指紋データ及び口座番号を登録するように構成したが、記憶装置２０４には、この他に、利用者の氏名、住所、電話番号、預金情報等の利用者個人の情報を記憶するようにしてもよい。これにより、振込サービスの利用時には、振込元の氏名、住所、電話番号が自動的に付加されるなど、種々のサービスに個人情報を利用することができる。

【００３０】

（第２の実施の形態）

次に、図４は第２の実施の形態を示すフローチャートであり、第２の実施の形態は、利用者の現金預け入れに対応する動作を示すものである。

利用者が自動現金受け払い機１０１に自身の現金を預け入れする場合は、ステップＳ２１で自身の預金通帳を差込口１０９に差し込む。ここで、利用者が自身の預金通帳に記帳が不要な場合はステップＳ２１の動作は省略される。続いて利用者は自身の所持する指紋認証トークン２００を差込口１０２に差込む（ステップＳ２２）。

【００３１】

すると、指紋認証トークン２００の処理装置２０３は、予め記憶装置２０４内に保存されているその利用者の銀行口座番号を自動現金受け払い機１０１の処理装置１０３に送信する（ステップＳ２３）。処理装置１０３は口座番号を受信すると、データベース１１０からこの口座番号に対応する残高を取得し記憶装置１０４に記憶する（ステップＳ２４）とともに、現金受け払い口１０６を開口する。この現金受け払い口１０６の開口により、利用者は自身の現金を現金受け払い

口１０６から入金する（ステップＳ２５）。

【００３２】

この場合、自動現金受け払い機１０１の処理装置１０３は、記憶装置１０４に保存されている利用者の残高にステップＳ２４で入金された金額を加算して、その合計金額を新たな残高として、データベース１１０の前記口座番号に対応して記録する（ステップＳ２６）。その後、利用者による指紋認証トークン２００の差込口１０２からの引き抜きが行われ（ステップＳ２７）、利用者の預金通帳が差し込まれている場合は、処理装置１０３は通帳記入装置１０８を制御して利用者の現金入金額などを預金通帳に記録させる（ステップＳ２８）。

【００３３】

なお、第２の実施の形態では、自動現金受け払い機１０１に指紋認証トークン２００が差し込まれると、指紋認証トークン２００は利用者の口座番号を自動現金受け払い機１０１側へ送信しているが、この場合、指紋センサ２０２で利用者の指紋画像を読み取り、読み取った指紋データと記憶装置２０４の登録指紋データとの一致に基づき利用者の口座番号を自動現金受け払い機１０１側へ送信するようにしても良い。このように構成することにより現金預入時のセキュリティが向上する。

【００３４】

以上、図３及び図４のフローチャートを参照して本発明の要部動作を説明したが、各ステップの実行順序を入れ替えても全体の動作に矛盾を生じない場合は各ステップの順序を適宜入れ替えてもよい。

また、本実施の形態では、自動現金受け払い機１０１による現金の引き出し及び現金の預け入れの各動作を説明したが、振り込みや振り替えなどの他のサービスに適用しても同等の効果を奏する。

また、本実施の形態では、指紋認証トークン２００を用いて本人認証を行うことにより、自動現金受け払い機の利用許可を与えているため、銀行カード及びパスワードが不要になり、セキュリティが向上する。

【００３５】

また、本実施の形態では、指紋認証トークン２００内の指紋センサ２０１，処

理装置２０３，記憶装置２０４をワンチップで構成した第１の構成例について説明したが、上記第１の構成例の他に、指紋センサ２０２をワンチップ化し、このワンチップ指紋センサ２０２に、バスを介して処理装置２０３を接続し、さらに処理装置２０３にバスを介して記憶装置２０４を接続する第２の構成例がある。さらに、指紋センサ２０２と処理装置２０３をワンチップ化し、このワンチップ化された処理装置２０３にバスを介して記憶装置２０４を接続する第３の構成例がある。

【００３６】

また、指紋認証トークン２００と自動現金受け払い機１０１間で送受される信号を送信側で暗号化し、受信側でその暗号化データを復号化することにより、システムのセキュリティを向上させることができる。

また、本実施の形態では、指紋の認証に基づいて現金の引き出しを行うようにしたが、指の大きさ、手形、静脈パターン、人相、虹彩及び声紋などの利用者固有の生体情報や、利用者のサイン（筆跡）等により利用者本人であることを認証して現金引き出しを許容するようにしても良い。

【００３７】

図７は、前述の指紋認証トークン２００を含む認証トークン３００と、認証トークン３００の認証を利用してユーザ（利用者）にサービスを提供する前述の自動現金受け払い機１０１を含む利用機器４００とからなる一般的な認証システムの構成を示すブロック図である。

この認証システムでは、ユーザ固有の生体情報として指紋を用いる場合を例として説明する。

【００３８】

認証トークン３００には、指紋（生体情報）を読み取るセンサ３１１（図２の指紋センサ２０２に対応）、ユーザ本人の登録指紋データ３１２Ａやユーザ情報３１２Ｂを記憶する記憶回路３１２（図２の記憶装置２０４に対応）、センサ３１１での読み取り結果を示すセンシングデータ３１１Ａを、記憶回路３１２に記憶されている登録指紋データ３１２Ａを用いて照合する照合回路３１３（図２の処理装置２０３に対応）、この照合回路３１３での照合結果を含む認証データ３

１３Ａを通信データ３０１Ａとして認証トークン３００の外部へ送信する通信回路３１４（図２の処理装置２０３に対応）が設けられており、これら回路部を一体として形成する認証トークン３００が利用機器４００に対して着脱自在に接続される。

利用機器４００には、認証トークン３００からの通信データ３０１Ａを受信する通信回路４２１と、受信した通信データ３０１Ａに含まれる照合結果が一致を示す場合にのみ、そのユーザへのサービス提供を行う処理装置４２２とが設けられている。

【００３９】

次に、図７に示す認証システムの動作について説明する。

ユーザは事前に、自分の所持する認証トークン３００の記憶回路３１２に、自分の登録指紋データ３１２Ａやサービスを利用するためのパスワードや個人情報などからなるユーザ情報３１２Ｂを記憶させておく。

利用機器４００を利用する際、まずユーザは自分の認証トークン３００を利用機器４００へ接続し、指をそのセンサ３１１へ置く。これにより認証トークン３００のセンサ３１１でユーザの指紋が読み取られセンシングデータ３１１Ａとして出力される。このセンシングデータ３１１Ａは照合回路３１３において記憶回路３１２の登録指紋データ３１２Ａを用いて照合される。そして、その照合結果を含む認証データ３１３Ａが出力される。このとき照合回路３１３は、予め記憶回路３１２に格納されているユーザＩＤ、パスワード、個人情報などのユーザ情報３１２Ｂを読み出し、認証データ３１３Ａへ含めて出力する。

【００４０】

通信回路３１４では、照合回路３１３からの認証データ３１３Ａを通信データ３０１Ａとして利用機器４００へ送信する。

利用機器４００の通信回路４２１では、認証トークン３００の通信回路３１４から送信された通信データ３０１Ａを受信し、認証データ３１３Ａと同じ内容の認証データ４２１Ａとして出力する。処理装置４２２では、この認証データ４２１Ａを受け取ってその認証データ４２１Ａに含まれる照合結果を参照する。そして、その照合結果が一致を示す場合、処理装置４２２においてユーザの所望する

所定の処理が実行される。

【００４１】

このように、ユーザの指紋を検出しその検出結果をセンシングデータとして出力するセンサ３１１と、ユーザの指紋を照合するための登録指紋データ３１２Ａが予め格納されている記憶回路３１２と、この記憶回路３１２に記憶されている登録指紋データ３１２Ａを用いてセンサ３１１からのセンシングデータ３１１Ａを照合し、ユーザ認証結果となるその照合結果を認証データとして出力する照合回路３１３と、この照合回路３１３からの認証データを通信データ３０１Ａとして利用機器４００へ送信する通信回路３１４とを、認証トークン３００として一体として形成したものである。

【００４２】

そして、認証に応じて所定の処理を行う利用機器４００をユーザが利用する場合には、認証トークン３００をその利用機器４００へ接続し、その認証トークン３００でユーザの生体情報に基づきユーザ認証を行い、利用機器４００へ通知するようにしたものである。

また、利用機器４００に、認証トークン３００から送信された通信データ３０１Ａを受信し認証データ４２１Ａとして出力する通信回路４２１と、この通信回路４２１からの認証データ４２１Ａに含まれる照合結果に基づき所定の処理を行う処理装置４２２とを設け、この利用機器４００とは独立した各ユーザが個々の持つ認証トークン３００での認証結果に基づき所定の処理を行うようにしたものである。

【００４３】

したがって、ユーザの生体情報を検出するセンサや照合を行う照合回路を利用機器内部に設け、ユーザの登録データをデータカードでユーザ自身が所持し管理する場合と比較して、登録データが認証トークンの外部へ出力されることがなくなり照合時に用いる登録データの漏洩を防止できる。また、センサを不特定多数のユーザで共用する必要がなく、ユーザが個々に所持する認証トークンごとに設けられているセンサを用いるため、センサ故障が発生しても他のユーザには波及せず、さらに生体情報検出の際、指紋などのようにセンサに対して人体の一部を

接触させる必要がある場合でもユーザに対して良好な衛生環境を保つことができる。なお、認証トークン３００については、センサ、記憶回路および照合回路などを１チップの半導体装置として形成する技術（例えば、特開２０００－２４２７７１号公報など参照）を用いることで、非常に小型な認証トークンを実現することも可能となる。

【００４４】

さらに、記憶回路３１２にユーザＩＤやパスワードさらには個人情報などのユーザ情報３１２Ｂを予め記憶しておき、これらを認証データ３１３Ａに含めて利用機器４００へ送信するようにしたので、利用機器４００の処理装置４２２において、その認証データに含まれるユーザ情報３１２Ｂ、例えばユーザＩＤやパスワードをチェックすることにより処理実行の可否を判断でき、利用機器で行う処理の重要性に合わせた基準で認証判定できる。また、ユーザ情報３１２Ｂの個人情報、例えば氏名、住所、電話番号、口座番号やクレジットカード番号などを処理に用いることにより、処理に必要な個人情報をユーザが入力する必要がなくなり、ユーザの操作負担を大幅に軽減できる。

【００４５】

なお、利用機器４００に図示しない乱数発生回路及び復号回路を設け、かつ認証トークン３００に図示しない暗号化回路を設けて、利用機器４００と認証トークン３００間で通信されるデータの暗号化することにより、セキュリティの向上を図ることができる。

【００４６】

即ち、利用機器４００は、認証トークン３００側からのアクセス時に乱数発生回路により乱数を発生させてこの乱数を通信回路４２１から認証トークン３００へ送信して暗号化回路に記憶させる一方、認証トークン３００の暗号化回路は照合回路３１３から出力された認証データ３１３Ａと、記憶した乱数との和を演算してその演算結果を、予め記憶回路３１２に記憶してある共通鍵により暗号化して暗号化データとして利用機器４００側へ送信する。利用機器４００では、通信回路４２１により受信したこの暗号化データを復号回路が共通鍵を用いて復号化するとともに復号化したデータから乱数発生回路が発生した前記乱数を減算する

ことにより認証データ４２１Ａとして処理回路４２２へ出力する。なお、上記の例では、認証トークン３００及び利用機器４００の双方に共通鍵を持たせて、それぞれ暗号化及び復号化を行わせているが、認証トークン３００に秘密鍵を、利用機器４００に公開鍵を持たせてそれぞれ暗号化処理及び復号化処理を行わせることもできる。

【００４７】

次に、図８を参照して、本認証システムの第２の構成例について説明する。図８は、図７に示す第１の構成例のうち、認証トークン３００の出力段にデータ変換モジュール３３０を付加したものである。

このデータ変換モジュール３３０には、認証トークン３００の通信回路３１４から出力された通信データを、利用機器４００で受信・解読可能なデータ形式へ変換するプロトコル変換回路３３１が設けられている。

【００４８】

このように、認証トークン３００に着脱自在に取り付けられるデータ変換モジュール３３０を介して、所望の利用機器４００と認証トークン３００とを接続するようにしたので、データ形式が異なる利用機器に対しても同一認証トークンを用いたユーザ認証が可能となる。また、様々な形式に対応したデータ変換モジュールを用意し、それらを認証トークンに対して容易に着脱交換することで、ユーザが１つの認証トークンを用いて様々な利用機器を利用することができ、複数の認証トークンを所持する必要がない。

以上では、データ変換モジュール３３０を認証トークン３００に対して着脱自在に取り付ける場合を例として説明したが、認証トークン３００内部にプロトコル変換回路３３１を設けてもよく、さらにコンパクトに構成できる。

【００４９】

次に、図９を参照して、本認証システムの第３の構成例について説明する。図９は、図７に示す第１の構成例のうち、認証トークン３００の出力段に無線モジュール３４０を付加したものである。

この無線モジュール３４０には、認証トークン３００の通信回路３１４から出力された通信データを、利用機器４００で受信・解読可能なデータ形式へ変換す

るプロトコル変換装置３４１と、このプロトコル変換装置３４１からの通信データを無線区間を介して利用機器４００へ送信する無線回路３４２とが設けられている。この場合、利用機器４００側にも無線回路４２３を設ける必要がある。

【００５０】

このように、認証トークン３００に着脱自在に取り付けられる無線モジュール３４０を用いて、所望の利用機器４００と認証トークン３００とを接続するようにしたので、ユーザは、認証トークン３００を利用機器４００に直接接続することなく、例えば自分の手元で認証トークン３００を用いてユーザ認証を行いサービスを受けることが可能となる。したがって、利用機器４００に対して認証トークン３００を接続する作業や、利用機器４００に接続されている状態の認証トークン３００を用いて認証を行う作業など、認証時のユーザに対する作業負担を大幅に軽減できる。

【００５１】

なお、利用機器４００と認証トークン３００の通信プロトコルが同一の場合は、無線モジュール３４０のプロトコル変換回路３４１を省略することも可能である。また、無線回路３４２の代わりに、赤外線通信回路や超音波通信回路など、無線区間を介してデータ通信可能な通信回路を用いてもよい。

以上では、無線モジュール３４０を認証トークン３００に対して着脱自在に取り付ける場合を例として説明したが、認証トークン３００内部に無線回路３４２やプロトコル変換回路３４１を設けてもよく、さらにコンパクトに構成できる。

【００５２】

【発明の効果】

以上説明したように本発明は、利用者の指紋画像等の生体情報の認証に基づき利用者に対しサービスを提供する生体情報認証自動現金受け払い機であって、利用者の生体情報に基づき利用者本人を認証する生体情報認証トークンを備え、前記生体情報認証トークンは利用者の生体情報を記憶する記憶手段と、利用者の生体情報を検出するセンサと、センサの検出情報と記憶手段の記憶情報との一致に基づき制御情報を出力する処理手段とを有し、処理手段の制御情報に基づき利用者に現金の受け払いを含む前記サービスを提供するようにしたので、従来の自動

現金受け払い機のように、利用者の登録指紋データが内部に読み込まれないため、指紋データが銀行側に悪用されるといった心配を利用者に抱かせるという問題を回避できる。また、従来の自動現金受け払い機のように、指紋センサを複数の利用者が共用で使用することがないことから、指紋センサ上の残存指紋が第三者により不正に利用されて容易に偽造指紋が作成されてしまうという問題も回避できる。

【図面の簡単な説明】

【図１】　本発明に係る自動現金受け払い機を適用したシステムの構成を示すブロック図である。

【図２】　前記自動現金受け払い機に用いられる指紋認証トークンの外観を示す図（図２（ａ））及びその構成を示すブロック図（図２（ｂ））である。

【図３】　現金引き出しの際の前記自動現金受け払い機及び指紋認証トークンの動作を示すフローチャートである。

【図４】　現金預け入れの際の前記自動現金受け払い機の動作を示すフローチャートである。

【図５】　前記指紋認証トークンを構成する指紋センサの詳細構成を示す図である。

【図６】　前記指紋センサ内の容量検出回路の回路図及び前記容量検出回路の各部の動作タイミングを示すタイムチャートである。

【図７】　認証トークンおよび利用機器からなる認証システムの第１の構成例を示すブロック図である。

【図８】　認証トークンおよび利用機器からなる認証システムの第２の構成例を示すブロック図である。

【図９】　認証トークンおよび利用機器からなる認証システムの第３の構成例を示すブロック図である。

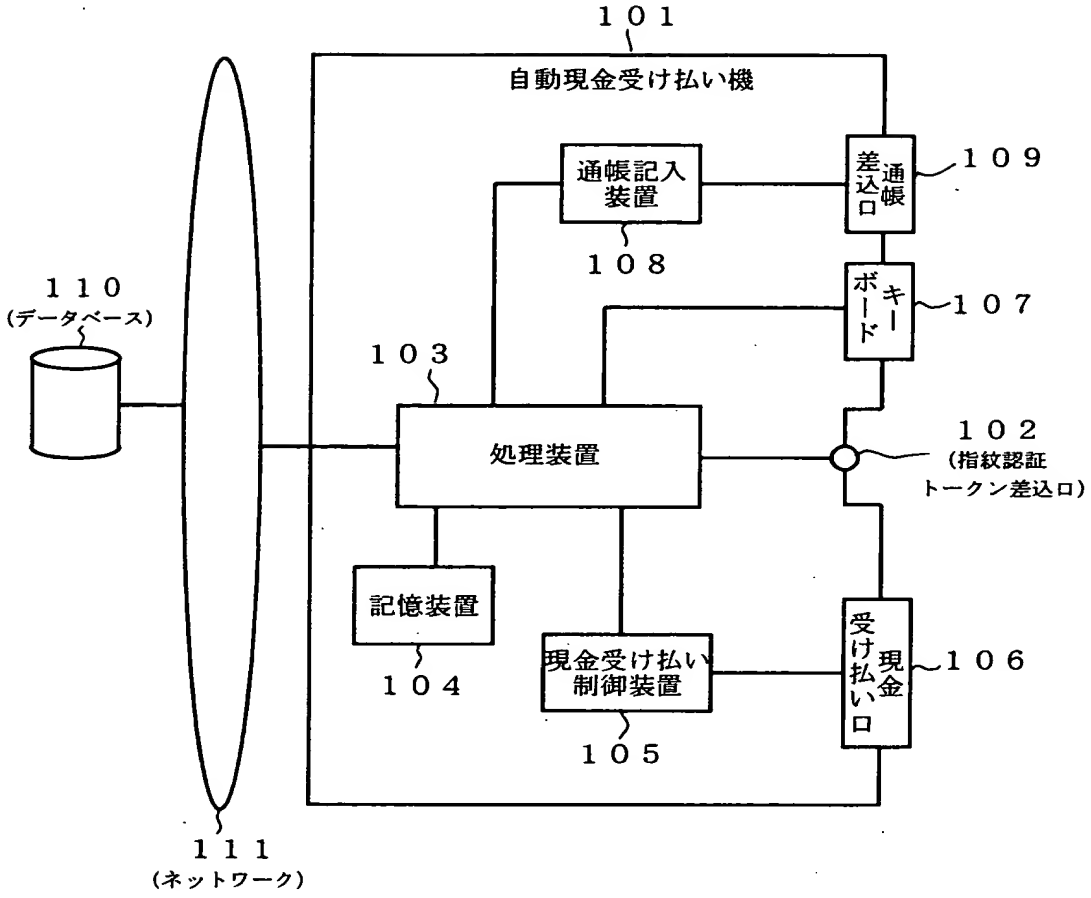
【符号の説明】

１０１…自動現金受け払い機、１０２…指紋認証トークン差込口、１０３，２０３…処理装置、１０４，２０４…記憶装置、１０５…現金受け払い制御装置、１０６…現金受け払い口、１０７…キーボード、１０８…通帳記入装置、１１０

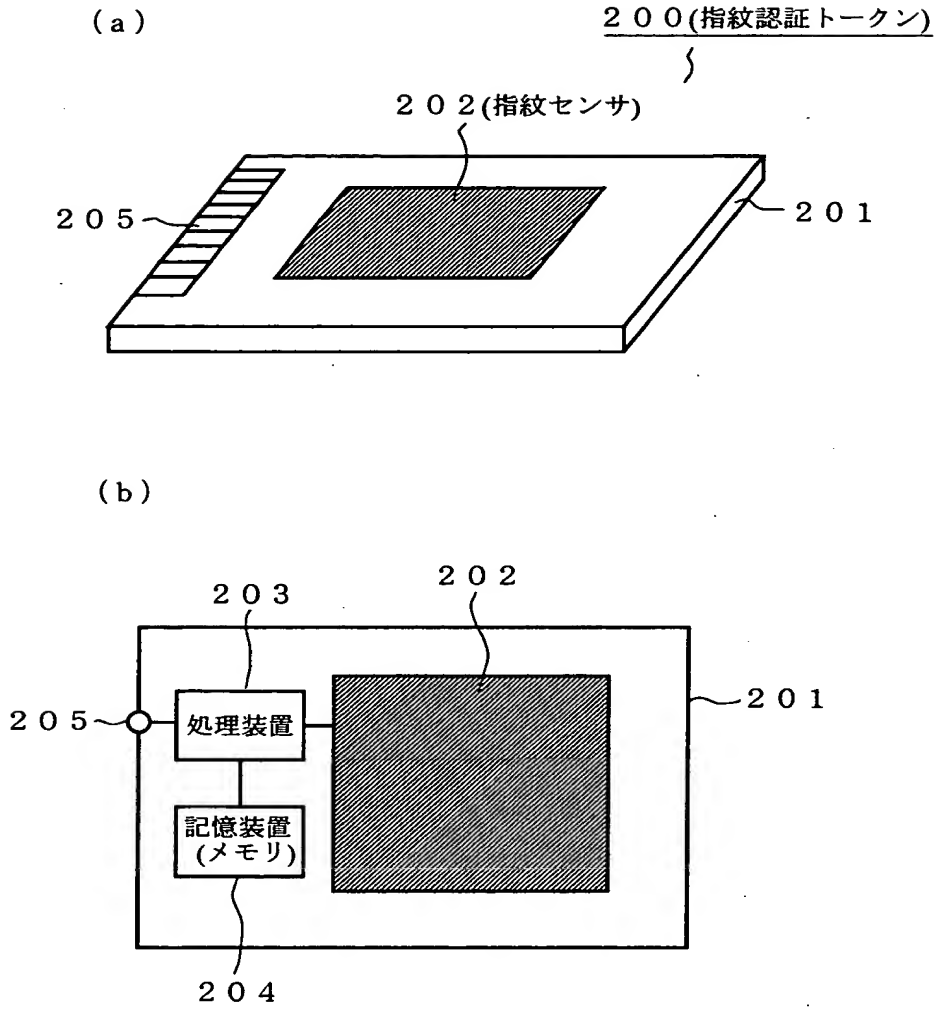
…データベース、２００…指紋認証トークン、２０２…指紋センサ、２０３…処理装置、２０４…記憶装置、２１１…半導体基板、２１２…下層絶縁膜、２１３…配線、２１４…層間絶縁膜、２１５…センサ電極、２１７…パシベーション膜、２１８…容量検出回路。

【書類名】　　図面

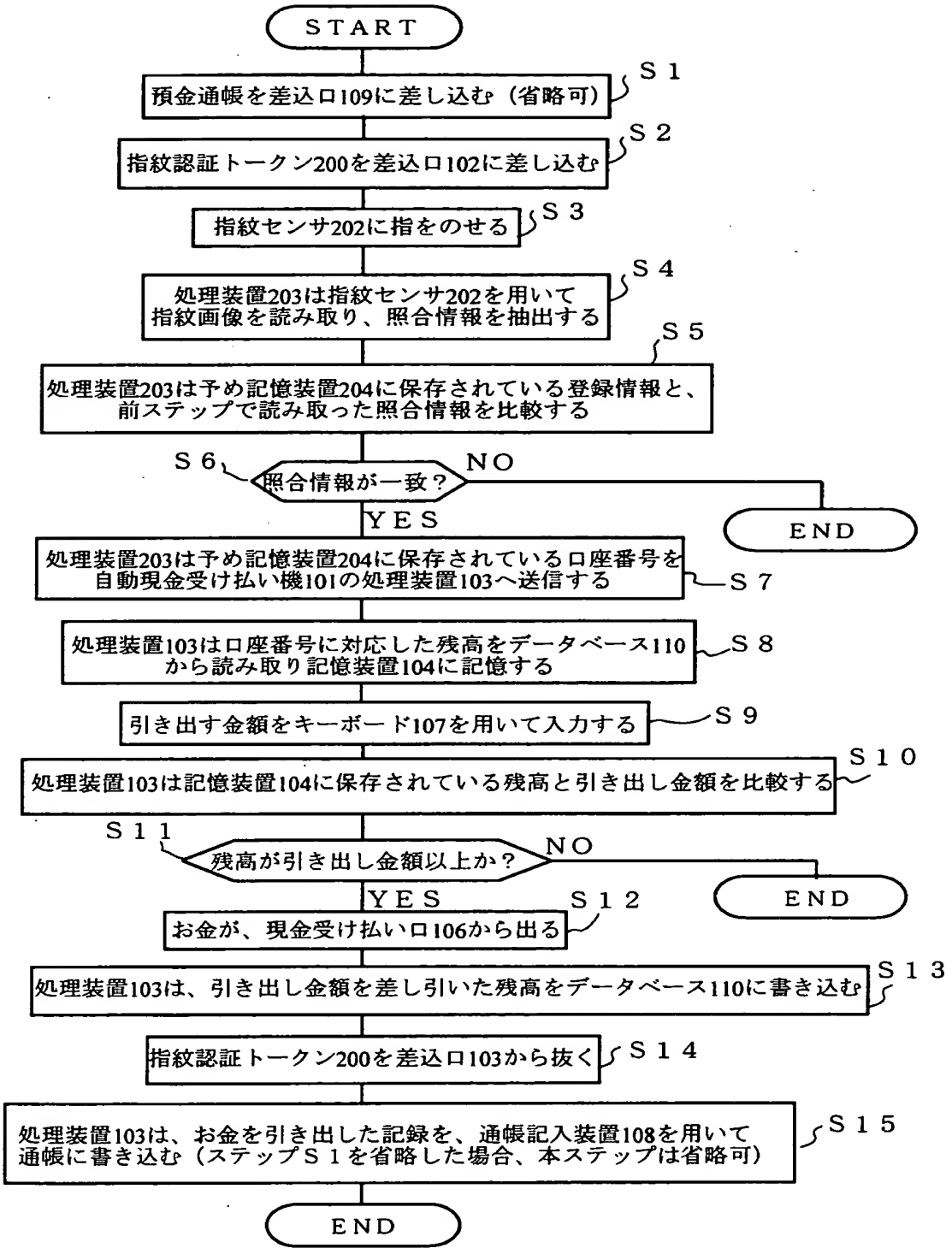
【図１】


１０１
自動現金受け払い機
通帳記入装置
１０８
差込口 通帳
１０９
キーボード
１０７
１０３
処理装置
１０２
（指紋認証
トークン差込口）
記憶装置
１０４
現金受け払い制御装置
１０５
受け払い口 現金
１０６
１１０
（データベース）
１１１
（ネットワーク）

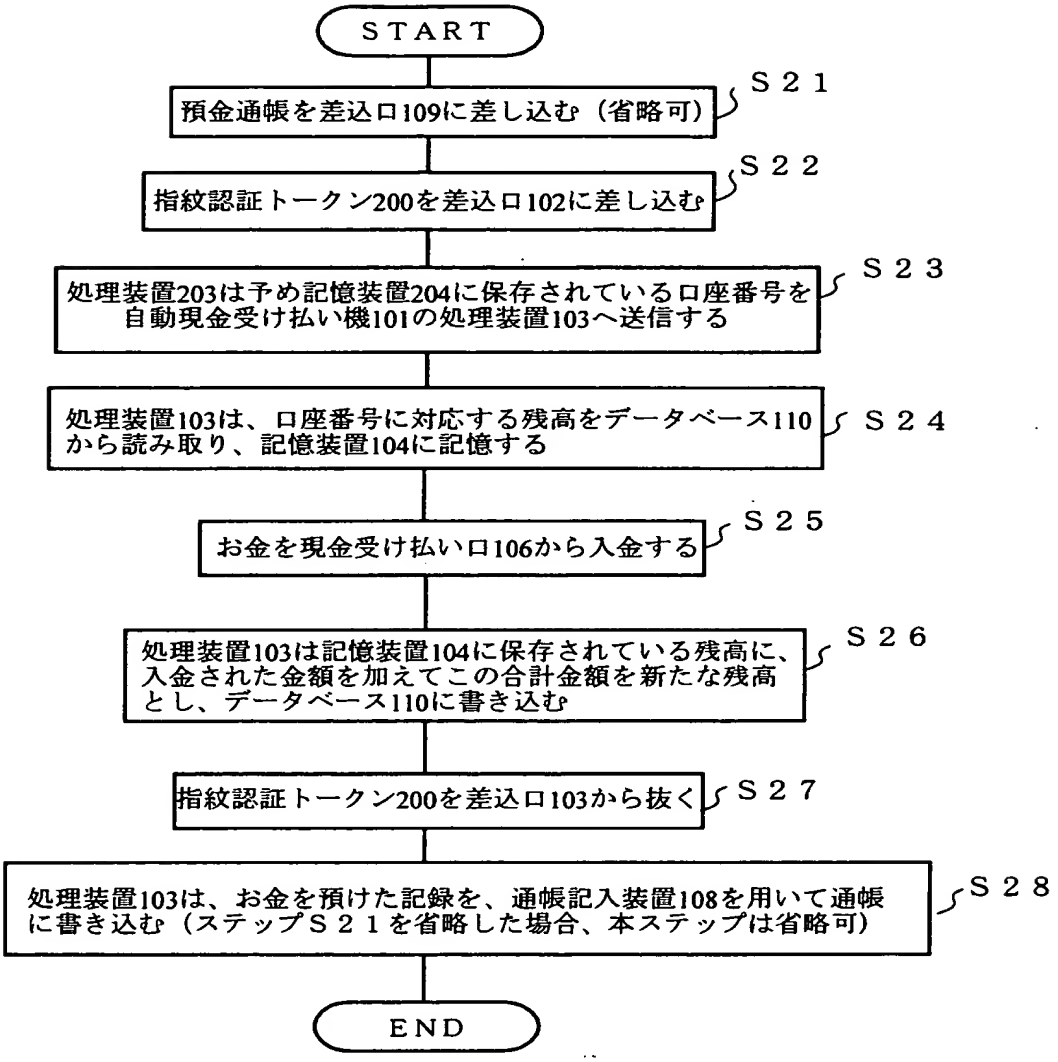
【図２】


（ａ）
２００(指紋認証トークン)
２０２(指紋センサ)
２０５
２０１
（ｂ）
２０３
２０２
２０５
処理装置
２０１
記憶装置
(メモリ)
２０４

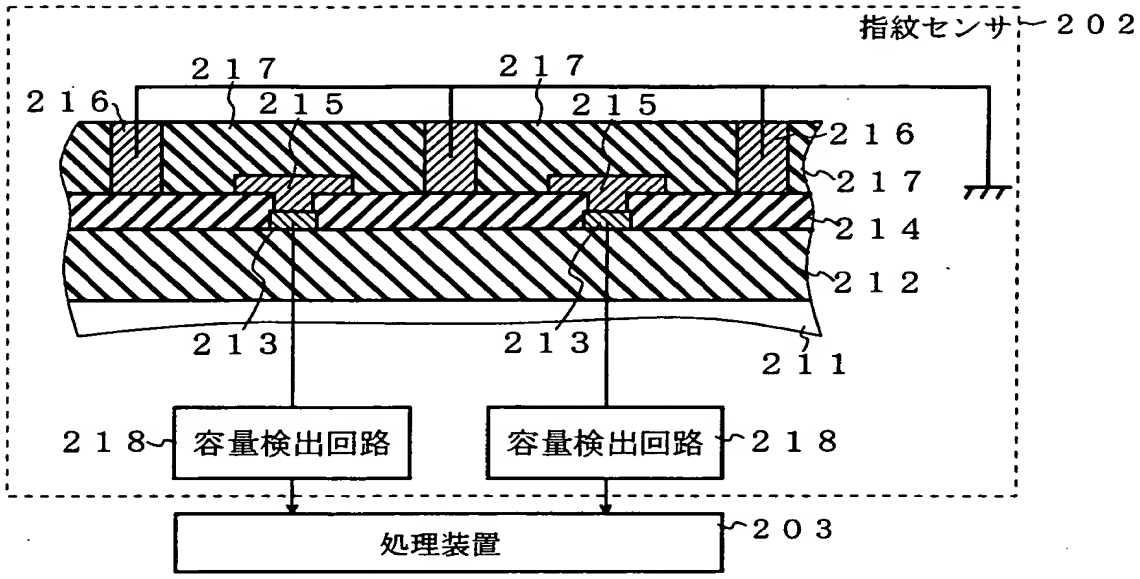
【図３】


START
預金通帳を差込口109に差し込む（省略可）
S１
指紋認証トークン200を差込口102に差し込む
S２
指紋センサ202に指をのせる
S３
処理装置203は指紋センサ202を用いて
指紋画像を読み取り、照合情報を抽出する
S４
処理装置203は予め記憶装置204に保存されている登録情報と、
前ステップで読み取った照合情報を比較する
S５
S６
照合情報が一致？
NO
END
YES
処理装置203は予め記憶装置204に保存されている口座番号を
自動現金受け払い機101の処理装置103へ送信する
S７
処理装置103は口座番号に対応した残高をデータベース110
から読み取り記憶装置104に記憶する
S８
引き出す金額をキーボード107を用いて入力する
S９
処理装置103は記憶装置104に保存されている残高と引き出し金額を比較する
S１０
S１１
残高が引き出し金額以上か？
NO
END
YES
S１２
お金が、現金受け払い口106から出る
処理装置103は、引き出し金額を差し引いた残高をデータベース110に書き込む
S１３
指紋認証トークン200を差込口103から抜く
S１４
処理装置103は、お金を引き出した記録を、通帳記入装置108を用いて
通帳に書き込む（ステップＳ１を省略した場合、本ステップは省略可）
S１５
END

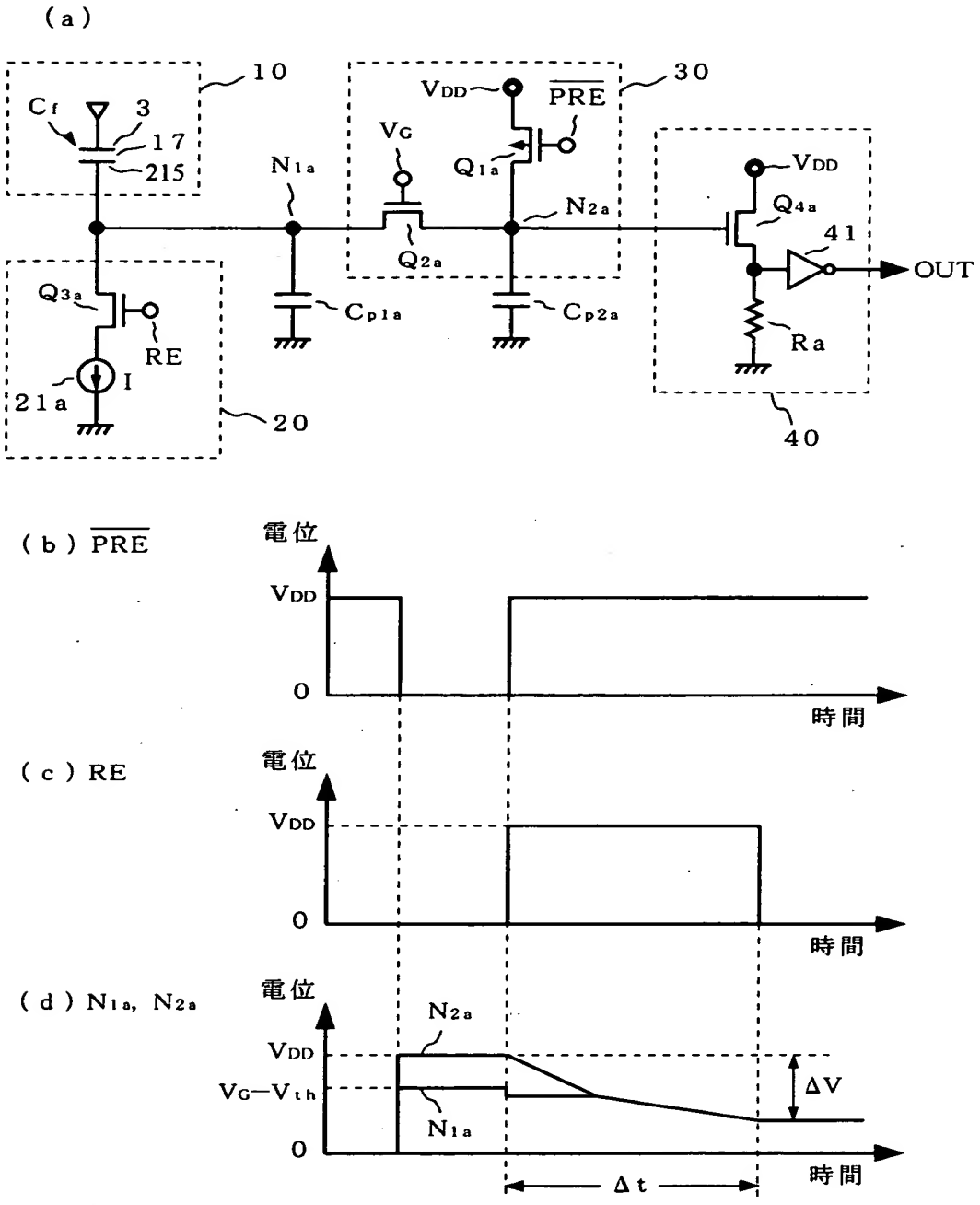
【図４】


START
預金通帳を差込口109に差し込む（省略可）
Ｓ２１
指紋認証トークン200を差込口102に差し込む
Ｓ２２
処理装置203は予め記憶装置204に保存されている口座番号を自動現金受け払い機101の処理装置103へ送信する
Ｓ２３
処理装置103は、口座番号に対応する残高をデータベース110から読み取り、記憶装置104に記憶する
Ｓ２４
お金を現金受け払い口106から入金する
Ｓ２５
処理装置103は記憶装置104に保存されている残高に、入金された金額を加えてこの合計金額を新たな残高とし、データベース110に書き込む
Ｓ２６
指紋認証トークン200を差込口103から抜く
Ｓ２７
処理装置103は、お金を預けた記録を、通帳記入装置108を用いて通帳に書き込む（ステップＳ２１を省略した場合、本ステップは省略可）
Ｓ２８
END

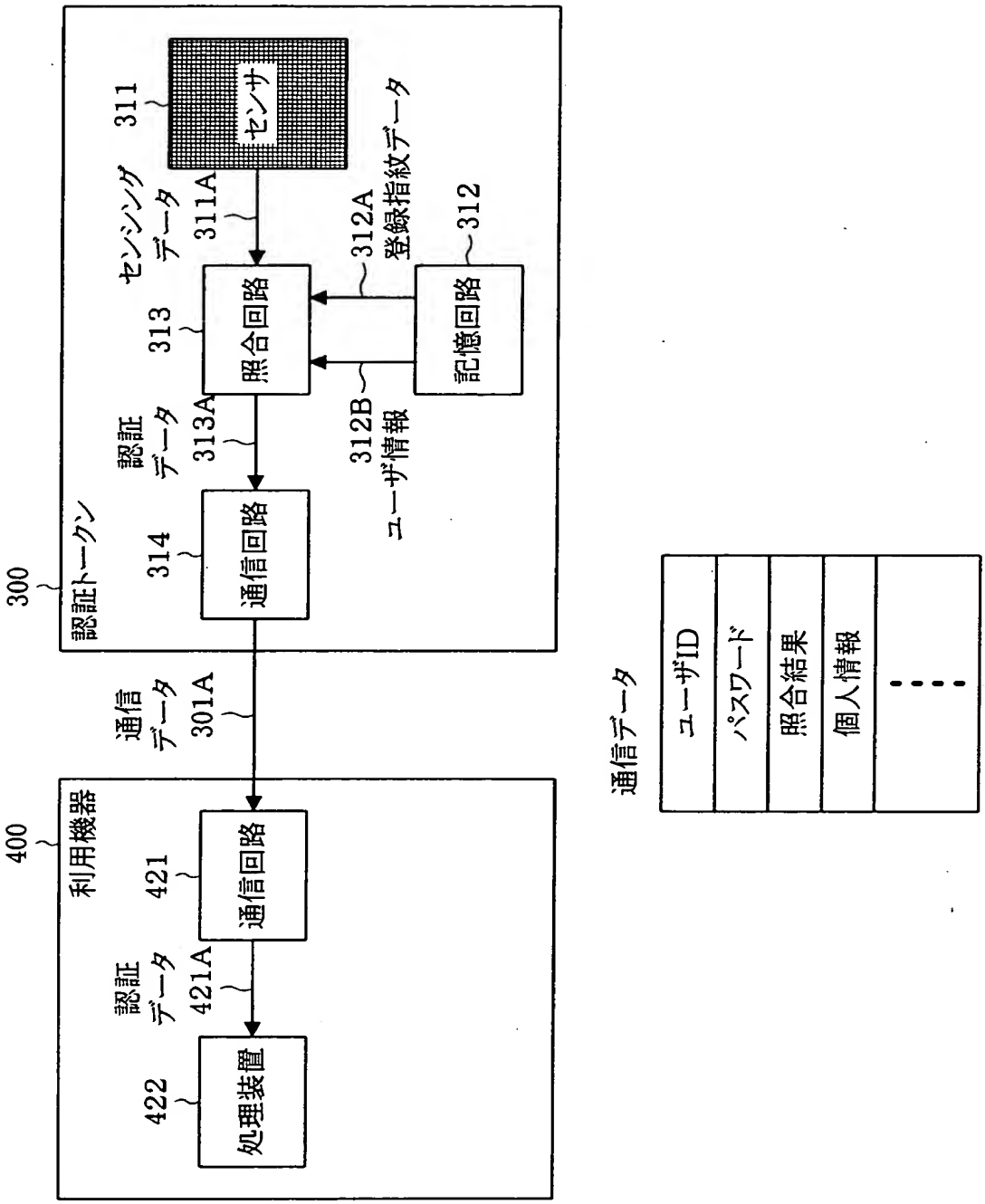
【図５】


指紋センサ
２０２
２１７
２１７
２１６
２１５
２１５
２１６
２１７
２１４
２１２
２１３
２１３
２１１
２１８
容量検出回路
容量検出回路
２１８
処理装置
２０３

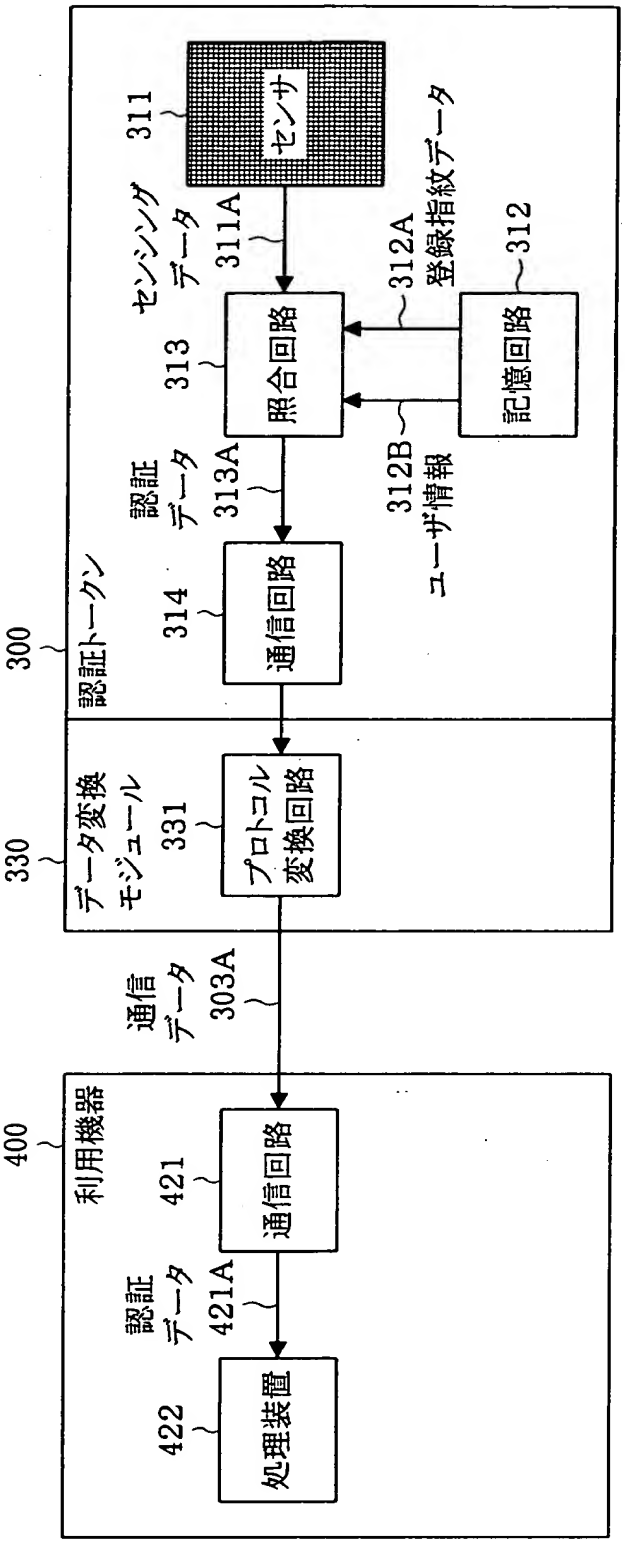
【図６】


(a)
10
Cf
3
17
215
N1a
VDD
PRE
30
VG
Q1a
N2a
Q2a
VDD
Q4a
41
OUT
Q3a
RE
I
21a
Cp1a
Cp2a
Ra
20
40
(b) PRE
電位
VDD
0
時間
(c) RE
電位
VDD
0
時間
(d) N1a, N2a
電位
N2a
VDD
VG−Vth
N1a
ΔV
0
Δt
時間

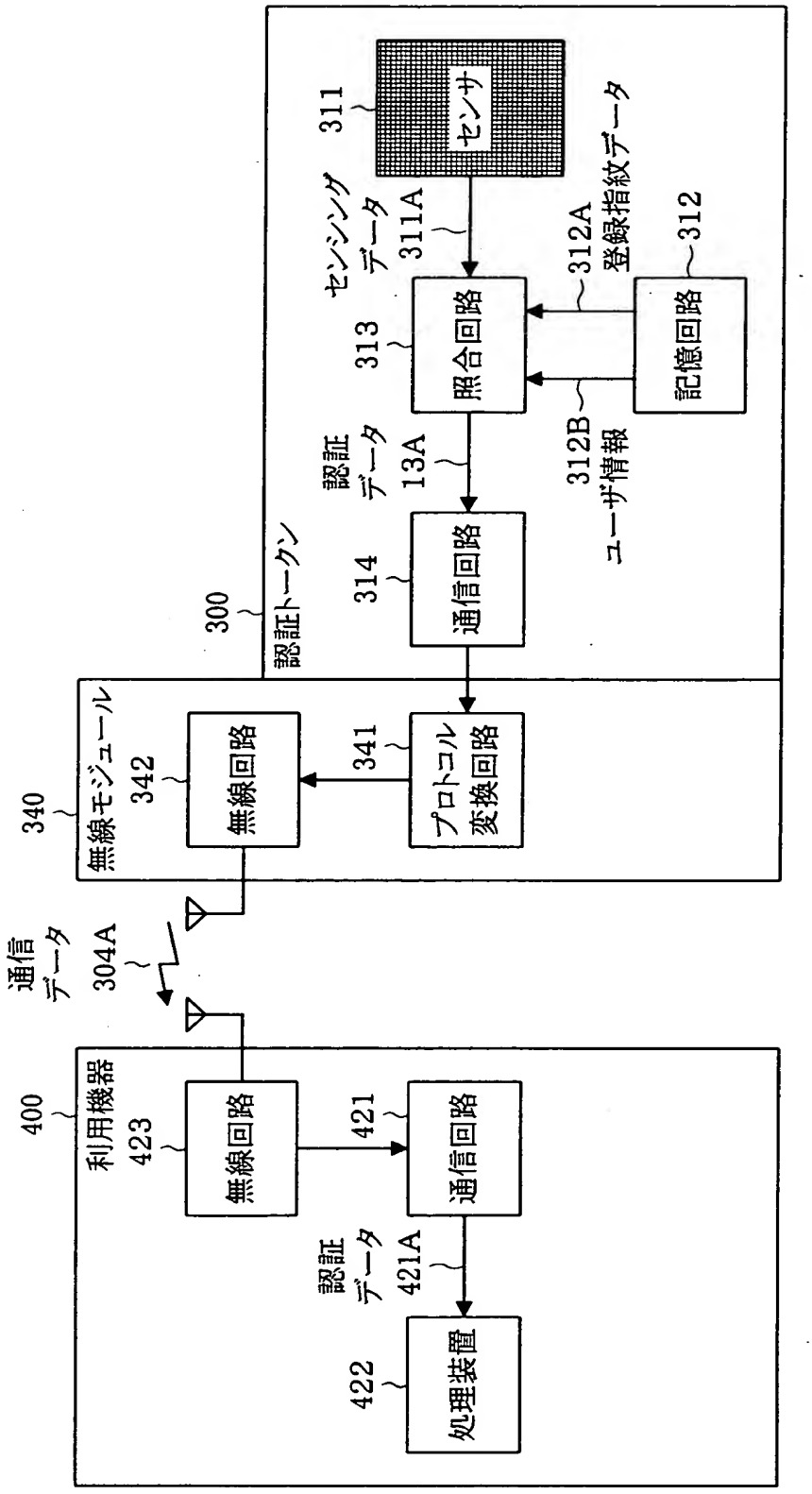
【図７】


300
認証トークン
311
センサ
センシングデータ
311A
312
312A
登録指紋データ
313
照合回路
記憶回路
認証データ
313A
312B
ユーザ情報
314
通信回路
通信データ
301A
400
利用機器
421
通信回路
認証データ
421A
422
処理装置
通信データ
ユーザID
パスワード
照合結果
個人情報

【図８】


センサ
311
センシングデータ
311A
312A
登録指紋データ
312
照合回路
313
記憶回路
認証データ
313A
312B
ユーザ情報
通信回路
314
認証トークン
300
データ変換モジュール
330
プロトコル変換回路
331
通信データ
303A
利用機器
400
通信回路
421
認証データ
421A
処理装置
422

【図９】


センサ
311
センシングデータ
311A
312A
登録指紋データ
312
照合回路
313
記憶回路
認証データ
13A
312B
ユーザ情報
通信回路
314
300
認証トークン
無線モジュール
340
無線回路
342
341
プロトコル変換回路
通信データ
304A
利用機器
400
無線回路
423
421
通信回路
認証データ
421A
処理装置
422

【書類名】　　要約書

【要約】

【課題】　利用者の指紋に基づき本人認証を行い利用者の現金の引き出しなど各種サービスを提供する場合、利用者の指紋データのセキュリティを向上させる。

【解決手段】　利用者が所有する指紋トークン200に利用者自身の指紋データを登録するとともに、利用者の口座番号を記憶し、指紋トークンの指紋センサ202が読み取った指紋データと登録データが一致すると、記憶している口座番号を自動現金受け払い機101へ送信し、自動現金受け払い機ではデータベース110からこの口座番号に対応する残高を取得しこの残高に応じた現金の払い出しを行う。

【選択図】　　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社